

(5) FOUO material transmitted outside the Department of Defense requires application of an expanded marking to explain the significance of the FOUO marking. This may be accomplished by typing or stamping the following statement on the record prior to transfer:

This document contains information
EXEMPT FROM MANDATORY DISCLOSURE
under the FOIA. Exemption(s) _____ applies/
apply.

(b) [Reserved]

§ 286.17 Dissemination and transmission.

(a) *Release and transmission procedures.* Until FOUO status is terminated, the release and transmission instructions that follow apply:

(1) FOUO information may be disseminated within DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized public disclosure. Transmittal documents shall call attention to the presence of FOUO attachments.

(2) DoD holders of FOUO information are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a government function, except to the extent prohibited by the Privacy Act. Records thus transmitted shall be marked "For Official Use Only," and the recipient shall be advised that the information may qualify for exemption from public disclosure, pursuant to the FOIA, and that special handling instructions do or do not apply.

(3) Release of FOUO information to Members of Congress is governed by DoD Directive 5400.4.⁹ Release to the GAO is governed by DoD Directive 7650.1.¹⁰ Records released to the Congress or GAO should be reviewed to determine whether the information warrants FOUO status. If not, prior FOUO markings shall be removed or effaced.

⁹See footnote 1 to § 286.1(a).

¹⁰See footnote 1 to § 286.1(a).

If withholding criteria are met, the records shall be marked FOUO and the recipient provided an explanation for such exemption and marking. Alternatively, the recipient may be requested, without marking the record, to protect against its public disclosure for reasons that are explained.

(b) *Transporting FOUO information.* Records containing FOUO information shall be transported in a manner that prevents disclosure of the contents. When not commingled with classified information, FOUO information may be sent via first-class mail or parcel post. Bulky shipments, such as distributions of FOUO Directives or testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail.

(c) *Electronically and facsimile transmitted messages.* Each part of electronically and facsimile transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text. Such messages and facsimiles shall be transmitted in accordance with communications security procedures whenever practicable.

§ 286.18 Safeguarding FOUO information.

(a) *During duty hours.* During normal working hours, records determined to be FOUO shall be placed in an out-of-sight location if the work area is accessible to nongovernment personnel.

(b) *During nonduty hours.* At the close of business, FOUO records shall be stored so as to prevent unauthorized access. Filing such material with other unclassified records in unlocked files or desks, etc., is adequate when normal U.S. Government or Government-contractor internal building security is provided during nonduty hours. When such internal security control is not exercised, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked receptacles such as file cabinets, desks, or bookcases. FOUO records that are subject to the provisions of the National Security

§ 286.19

Act of 1959 shall meet the safeguards outlined for that group of records.

§ 286.19 Termination, disposal and unauthorized disclosure.

(a) *Termination.* The originator or other competent authority; e.g., initial denial and appellate authorities, shall terminate “For Official Use Only” markings or status when circumstances indicate that the information no longer requires protection from public disclosure. When FOUO status is terminated, all known holders shall be notified, to the extent practical. Upon notification, holders shall efface or remove the “For Official Use Only” markings, but records in file or storage need not be retrieved solely for that purpose.

(b) *Disposal.* (1) Nonrecord copies of FOUO materials may be destroyed by tearing each copy into pieces to prevent reconstructing, and placing them in regular trash containers. When local circumstances or experience indicates that this destruction method is not sufficiently protective of FOUO information, local authorities may direct other methods but must give due consideration to the additional expense balanced against the degree of sensitivity of the type of FOUO information contained in the records.

(2) Record copies of FOUO documents shall be disposed of in accordance with the disposal standards established under 44 U.S.C. 3301-3314, as implemented by DoD Component instructions concerning records disposal.

(c) *Unauthorized disclosure.* The unauthorized disclosure of FOUO records does not constitute an unauthorized disclosure of DoD information classified for security purposes. Appropriate administrative action shall be taken, however, to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

32 CFR Ch. I (7-1-05 Edition)

Subpart E—Release and Processing Procedures

§ 286.22 General provisions.

(a) *Public information.* (1) Since the policy of the Department of Defense is to make the maximum amount of information available to the public consistent with its other responsibilities, written requests for a DoD record made under the provisions of 5 U.S.C. 552(a)(3) of the FOIA may be denied only when:

(i) Disclosure would result in a foreseeable harm to an interest protected by a FOIA exemption, and the record is subject to one or more of the exemptions of FOIA.

(ii) The record has not been described well enough to enable the DoD Component to locate it with a reasonable amount of effort by an employee familiar with the files.

(iii) The requester has failed to comply with the procedural requirements, including the written agreement to pay or payment of any required fee imposed by the instructions of the DoD Component concerned. When personally identifiable information in a record is requested by the subject of the record or the subject's attorney, notarization of the request, or a statement certifying under the penalty of perjury that their identity is true and correct may be required. Additionally, written consent of the subject of the record is required for disclosure from a Privacy Act System of records, even to the subject's attorney.

(2) Individuals seeking DoD information should address their FOIA requests to one of the addresses listed in appendix B of this part.

(b) *Requests from private parties.* The provisions of the FOIA are reserved for persons with private interest as opposed to U.S. Federal Agencies seeking official information. Requests from private persons will be made in writing, and should clearly show all other addressees within the Federal Government to which the request was also sent. This procedure will reduce processing time requirements, and ensure better inter- and intra-agency coordination. However, if the requester does not show all other addressees to which